Futurum

DELL Technologies

Building Optimal Cyber Resilience with All-Flash Protection Infrastructure

MAY 2025

Introduction

The need to optimize IT resources and otherwise cut costs is always a top priority. While budget constraints will always be present, the onslaught of cyberattacks has given precedence to optimizing cyber resilience to avoid and mitigate business disruption and loss of sensitive and critical data.

Key Insights from The Futurum Group's 1H 2025 Cybersecurity Decision Maker Study

1 in 5 decision-makers prioritize stricter RPO and RTO goals as their top initiative in data security.

< 10% focus on reducing Total Cost of Ownership (TCO)

A challenge facing practitioners as they work to optimize cyber resilience for their organization is the intersection point of traditional and modern workloads, such as artificial intelligence (AI) and cloud-native applications. This adds complexity and creates new requirements, including the need to support bare metal, virtual machine, and container environments alike, the need for a consistent, shared data layer, and the need to avoid vendor lock-in.

What Is Cyber Resilience?

At the end of the day, cyber resilience is the ability to withstand and recover quickly from a destructive cyber attack—and meeting stringent recovery point and recovery time objectives is a key factor for any organization. The priority is getting critical services back online as soon as possible following a data breach and mitigate—or entirely avoid, when possible—the loss of the organization's most critical and sensitive data. Given the precedence on RPO and RTO that this creates, recovery is a vital component to getting back up and running as quickly as possible should an issue occur.

Furthermore, embracing cyber resilience shifts the strategy to being more proactive, assuming that there will ultimately be malicious access. Specifically, this encompasses preventing malicious tampering with data and identifying potentially nefarious activity in order to limit the spread of attacks and to respond more quickly.

Key Criteria for Cyber Resilience Infrastructure

All-Flash for Faster Recoveries: Not All Systems Were Created Equal

When it comes to leveraging backup and recovery infrastructure to build a foundation for cyber resilience, optimizing the speed of data ingestion and recovery performance is fundamental. Doing so helps to ensure that backups are successfully completed within the required backup window, as a result optimizing the number of available recovery points and helping to reduce the amount of potential data loss. It is also important when it comes to completing recovery operations as quickly as possible, in turn mitigating downtime.

The precedence on performance has created a use case for all-flash-based data protection systems. However, not all flash storage systems are created equal. It is important to evaluate offerings beyond the performance of the flash drive itself, carefully considering the architecture of the storage array comprehensively from the standpoint of its additional complementary security, durability, efficiency, and flexibility capabilities.

For security, notably, this includes the ability to create immutable data copies, in order to prevent changes from being made to data copies. However, sophisticated cyber attackers may still attempt to compromise or render inaccessible even immutable data copies through techniques such as destroying access keys or encrypting the immutable storage. As a result, the ability to conduct end-to-end validation to ensure that data copies are clean and recoverable, not corrupted or otherwise tampered with, is also important.

End-to-end data encryption is also table stakes, acting as a critical barrier against malicious tampering by rendering data unintelligible to unauthorized parties, in transit, at rest, and while in use. Even if attackers were to gain access to data stores or intercept communications, the encryption layer inhibits their ability to understand or modify sensitive information without the correct decryption keys, thus bolstering data confidentiality and integrity.

Hardware Root of Trust (HRoT) and Secure Boot also move the needle when it comes to cyber resilience for data protection systems by establishing an immutable hardware-based chain of trust during the boot process. This prevents pre-boot malware such as bootkits and rootkits, ensures the integrity and authenticity of loaded software, and protects sensitive cryptographic keys through secure storage and potentially Trusted Execution Environments.

It is relevant to note that SSDs offer greater efficiencies for rack space and power savings compared to hard disk drives, which can be augmented by data reduction capabilities. This materially increases cost savings over the lifetime of the storage system, especially when it comes to protecting and recovering business-critical data and IT services.

Beyond Flash: Additional Considerations for Cyber Resilience

Given the sophisticated nature of attacks, it is inevitable that data breaches will occur. To that end, using AI and ML to detect anomalous and potentially malicious activity becomes an important check box in order to reduce the spread of attacks. Furthermore, the ability to create an isolated and air-gapped "cyber vault" environment helps to securely store and protect critical data copies. This approach minimizes the attack surface and prevents ransomware or other cyber threats from reaching backup data, ensuring a reliable and rapidly recoverable data asset in the event of a successful attack. Additionally, it provides a clean and isolated environment for forensic analysis.

Finally, enterprises use a variety of data protection software offerings, in order to meet the backup and recovery requirements for their range of applications, infrastructures, and workloads. When it comes to an infrastructure provider, the ability to support these multiple platforms therefore also becomes important.

Enter Dell PowerProtect Data Domain All-Flash Appliance and Data Services

Figure 1: PowerProtect Data Domain Platform

Source: Dell Technologies

Cybersecurity has become a top-level concern for enterprise IT organizations, not only because of the increasing frequency and sophistication of attacks, but because the consequences of data loss or extended downtime are more severe than ever. In response, the conversation around cyber resilience has evolved. No longer is the focus solely on having backups; it is on how fast, how accurately, and how confidently those backups can be restored in the face of an incident, and in particular in the likely event of a cyber incident.

In this context, cyber resilience has emerged as a strategic imperative. Enterprises are now building layered defense and recovery strategies that combine proactive threat mitigation with reliable post-incident restoration capabilities. While HDD-based systems continue to serve an essential role, organizations are increasingly looking toward all-flash backup appliances to address specific needs around speed and complementary capabilities for data verification and operational efficiency.

Dell Technologies' PowerProtect Data Domain All-Flash appliance represents a direct response to this shift by strengthening an organization's overall resilience posture. This analysis explores how the Data Domain All-Flash appliance and Data Domain Platform data services can help IT leaders close critical gaps in their cyber recovery strategy, particularly in sectors with regulatory oversight, performance sensitivity, or constrained operational environments.

Key Takeaways

1) Comprehensive security is foundational to cyber recovery readiness.

The Data Domain All-Flash appliance introduces a layered approach to protection through security capabilities designed to safeguard backup data throughout its lifecycle. Immutable data copies are a key component, preventing alterations to backup sets and providing a baseline for recovery. Data Domain's immutability is compliance-grade, deduplication-aware, and enforced at the storage layer—delivering tamper-resistant protection that is more difficult to bypass than software-defined alternatives, without a penalty to storage performance.

The appliance further enhances resilience through end-to-end encryption of data in transit, at rest, and even during use. This renders backup data unintelligible to unauthorized actors, even in the event of storage compromise or intercepted communication.

At the hardware level, features like Secure Boot and Hardware Root of Trust (HRoT) establish a cryptographic chain of trust from the moment the system powers on. These capabilities help ensure that only verified software is loaded and that sensitive cryptographic keys are securely stored, reducing exposure to pre-boot malware such as rootkits and bootkits.

Additional safeguards include the option to create an isolated cyber recovery vault, physically or logically isolating backup data from production environments. This model minimizes attack surfaces and ensures that at least one clean, untouchable recovery copy exists, even in the event of a widespread breach. Collectively, these capabilities move the appliance beyond traditional backup, positioning it to address modern cyber resilience requirements.

2) Recovery performance addresses business-level concerns.

IT leaders understand that recovery speed is no longer just a technical metric—it's a direct contributor to business continuity. Dell's Data Domain All-Flash appliance incorporates a data service called DD Boost, which offloads deduplication processing to the source. This design minimizes data movement and system overhead, significantly improving restore times. Dell claims up to 4x faster restores and 2x faster replication compared to comparable HDD-based systems. When a cyber incident occurs, rapid restoration of critical applications can determine how quickly operations return to normal. As recovery time objectives (RTOs) become shorter across industries, fast-restore capabilities are no longer a luxury—they are foundational.

3) Infrastructure efficiency is an increasingly strategic consideration.

As data centers seek to reduce energy consumption, improve space utilization, and simplify operations, efficiency and the ability to measurably reduce infrastructure overhead have become a core metric for evaluating cyber resilience solutions. Compared to HDD-based solutions, Dell reports a 40% reduction in rack space requirements and up to 80% lower power consumption, while delivering typically 65:1 data reduction.

4) Data integrity verification is a core resilience feature.

One of the most significant—and often underappreciated—challenges during a cyber incident is the risk of restoring compromised or corrupted data. In response, leading vendors are building in capabilities that go beyond traditional backup. Dell's Data Invulnerability Architecture offers continuous verification of backup data during the protection process. This provides IT teams with higher assurance that restored data is clean and reliable. In an age of sophisticated cyber threats, confidence in the integrity of recovery points is as important as the backups themselves.

5) Interoperability as a key factor in enterprise decision-making.

Finally, the value of any data protection solution is significantly enhanced by its ability to fit into diverse and often complex IT ecosystems. The Data Domain All-Flash appliance supports broad integration with third-party backup software through the DD Boost ecosystem, making it easier to incorporate into existing operational workflows. For enterprises that have already invested in Dell's primary storage platforms—such as PowerMax or PowerStore—the native integration across platforms simplifies coordination between production and protection infrastructure. This level of interoperability helps organizations reduce complexity and maximize the value of their broader IT investments.

Conclusion: An All-Flash Approach to a Resilient Future

The growing sophistication of cyber threats and the tightening of regulatory frameworks are changing how enterprises approach backup and recovery. Organizations are increasingly looking to all-flash appliances to address the high-performance, high-assurance demands of modern cyber resilience.

With the introduction of the PowerProtect Data Domain All-Flash appliance, Dell is bringing proven Data Domain capabilities to a significantly higher performance, power-efficient all-flash form factor. This evolution gives customers the opportunity to leverage Data Domain's broad security, data deduplication, and data integrity capabilities, alongside its broad ecosystem integration, while also capitalizing on the improved performance, space, and energy benefits unique to flash storage.

As cybersecurity concerns continue to move from a back-office function to a boardroom priority, solutions like the Data Domain All-Flash appliance will play a growing role in how enterprises secure, detect, and recover.

Learn more here:

- Futurum – Fireside Chat video
- PowerProtect Data Domain All-Flash appliance video
- PowerProtect Data Domain Platform infographic

Important Information About This Report

AUTHORS

Krista Case
Research Director, Cybersecurity | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DELL Technologies

ABOUT DELL TECHNOLOGIES

Dell Technologies is a global leader in IT infrastructure, offering a comprehensive portfolio of solutions that help organizations store, protect, and manage data across hybrid and multicloud environments. At the forefront of its cyber resilience lineup is Dell PowerProtect Data Domain, a trusted platform known for its high-performance deduplication, scalability, and security capabilities. This solution helps enterprises safeguard critical workloads, reduce storage costs, and accelerate recovery times.

Futurum

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

Futurum
CONTACT INFORMATION: The Futurum Group LLC | futurumgroup.com | (833) 722-5337